

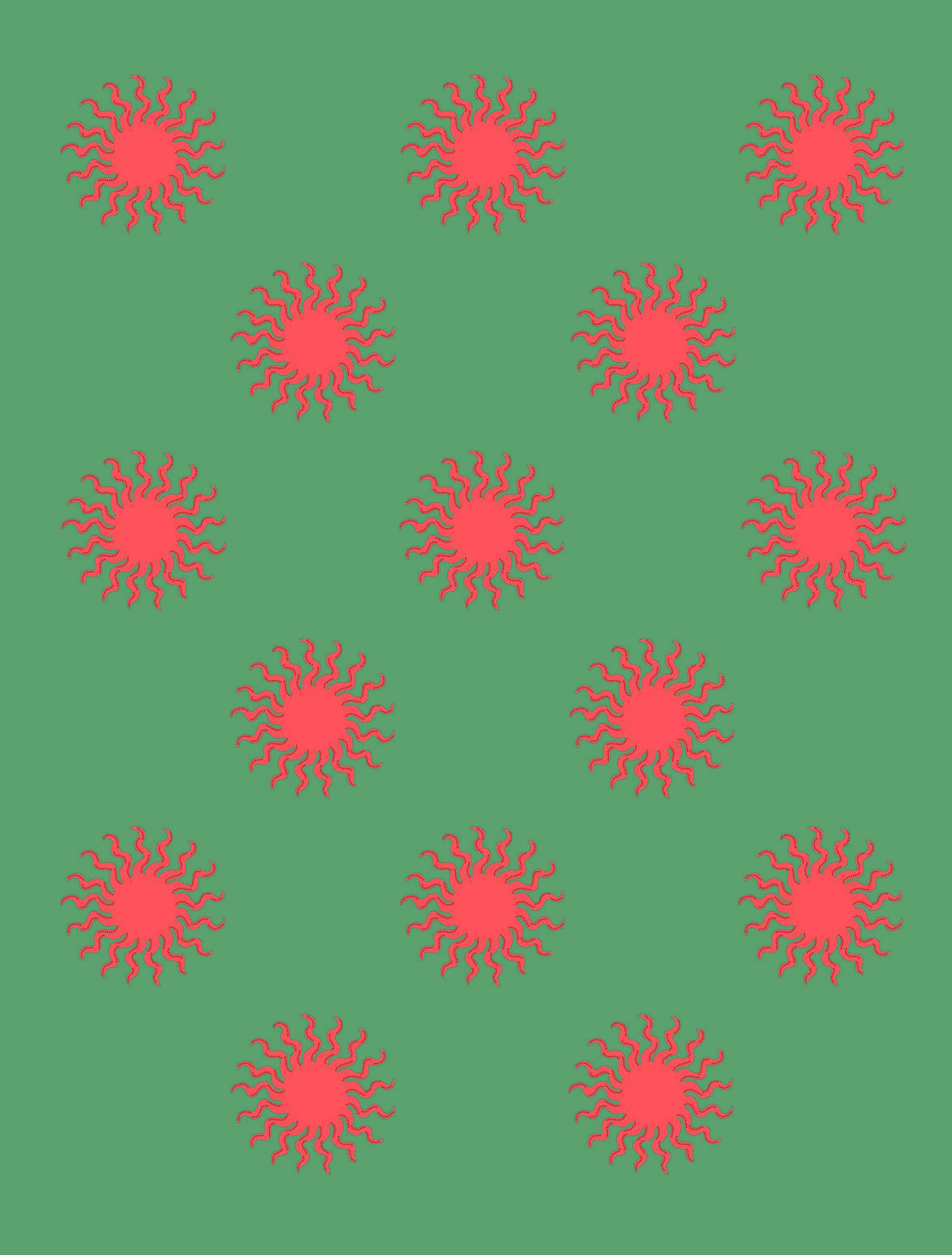
ENTRE DESCONEXIONES Y RIESGOS:

seguridad digital para las personas defensoras de los derechos humanos en Colombia.

Experiencia de un centenar de ellas

<K+LAB>

Fundación Karisma



Bogotá, Colombia
Noviembre, 2024

Autor
Nicholas Guecha

Con el apoyo de
Angie Ballesteros
Lorena Enciso

Revisado por
Carolina Botero
Catalina Moreno

Dirección Fundación Karisma
Catalina Moreno Arocha
Juan Diego Castañeda

Coordinación editorial
Natalia Andrade Fajardo

Diseño editorial
Natalia Noriega Gómez

Identidad gráfica
Daniela Moreno Ramírez



En un esfuerzo para que todas las personas tengan acceso al conocimiento, la Fundación Karisma está trabajando para que sus documentos sean accesibles. Esto quiere decir que su formato incluye metadatos y otros elementos que lo hacen compatible con herramientas como lectores de pantalla o pantallas braille. El propósito del diseño accesible es que todas las personas, incluida las que tienen algún tipo de discapacidad o dificultad para la lectura y comprensión, puedan acceder a los contenidos.



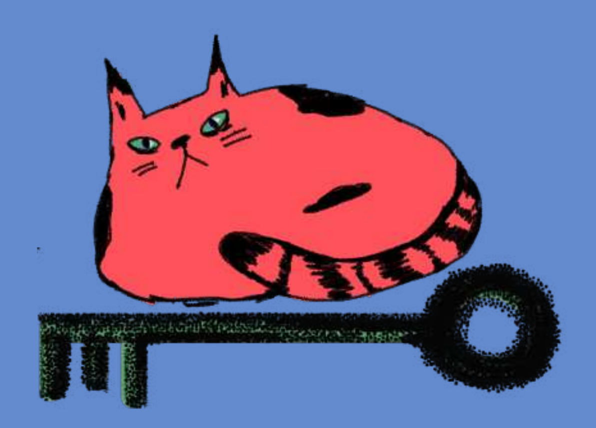
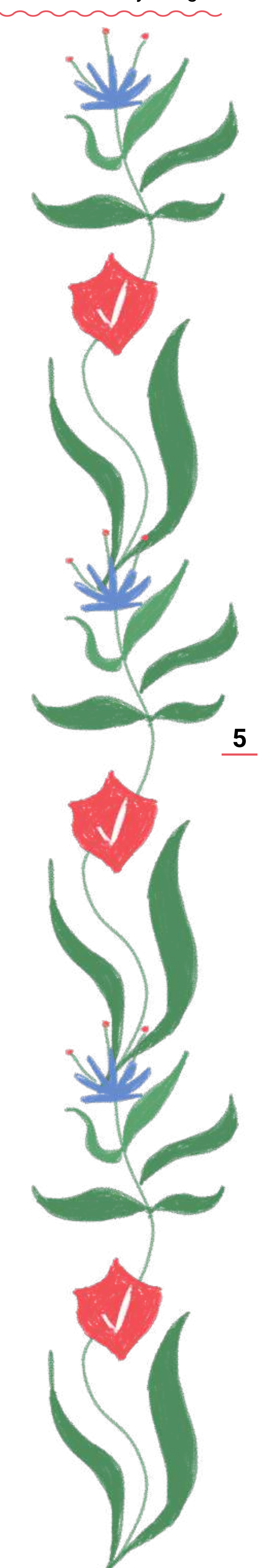


Tabla de Contenidos



00. Resumen ejecutivo

El informe Seguridad digital y riesgos digitales para personas defensoras de derechos humanos en Colombia analiza la experiencia de más de cien personas defensoras de derechos humanos respecto al uso y los riesgos asociados a las tecnologías digitales en su labor. Se utilizan metodologías mixtas, combinando encuestas y grupos focales para evaluar la apropiación digital, el acceso a internet y los incidentes de seguridad digital que enfrentan estas personas.

Principales hallazgos

1

Apropiación digital:

El 72 % de los defensores tiene niveles bajos o medios de apropiación digital. Esto significa que pocos han integrado plenamente las herramientas digitales en sus labores, lo que podría aumentar los riesgos de seguridad digital.

2

Acceso a internet:

Si bien la mayoría tiene acceso a internet, las personas en zonas rurales enfrentan mayores desigualdades, con menor acceso a planes de datos o internet en el hogar, lo que limita su capacidad de conectarse de manera segura.

3

Riesgos de seguridad digital:

La encuesta revela que muchas personas defensoras no toman medidas de protección básicas, como cambiar contraseñas de redes wifi o hacer copias de seguridad de información. Además, los niveles de apropiación digital no se identifican como el principal factor que reduce los riesgos digitales, lo que sugiere que la falta de formación y protocolos es un problema mayor.



Incidentes digitales:

Los ataques más reportados incluyen acceso no autorizado a dispositivos, phishing y suplantación de identidad. Además, el 50 % de las personas encuestadas ha recibido amenazas a través de medios digitales.

Recomendaciones

El informe resalta la necesidad de mejorar la formación en seguridad digital y de crear estrategias que permitan a las personas defensoras adoptar medidas de protección más efectivas, especialmente en áreas rurales.

Este documento subraya la importancia de garantizar un entorno digital seguro para quienes trabajan en la defensa de los derechos humanos, considerando las vulnerabilidades tecnológicas a las que están expuestas.

01. Introducción

En Colombia, las personas defensoras de derechos humanos desempeñan un papel fundamental en la promoción y protección de los derechos fundamentales, tanto a nivel local como nacional. Estas personas, que pueden pertenecer a diversas profesiones, edades y géneros, enfrentan una serie de desafíos y riesgos asociados con su labor, particularmente en contextos de violencia, marginalización y falta de acceso a protección adecuada. **La relevancia de su trabajo se refleja en la amplia definición que se les adjudica tanto a nivel internacional como local, dado que su identidad se construye a partir de las acciones que realizan en defensa de los derechos humanos, muchas veces vinculadas a liderazgos comunitarios y sociales.**

Sin embargo, en el país las personas defensoras continúan enfrentando condiciones precarias que ponen en riesgo su seguridad, a lo cual se suman las amenazas digitales que han emergido en la última década, ampliando el alcance de las violencias y acciones que buscan entorpecer o limitar sus actividades.

Con el aumento del uso de tecnologías digitales, la apropiación de estas herramientas se ha convertido en un componente clave para la labor de los defensores de derechos humanos. Este proceso de apropiación digital, que va más allá de la simple popularización y divulgación de tecnologías, implica que las personas defensoras sean agentes activos en el uso y la adaptación de herramientas digitales para satisfacer sus necesidades particulares y las de sus comunidades.

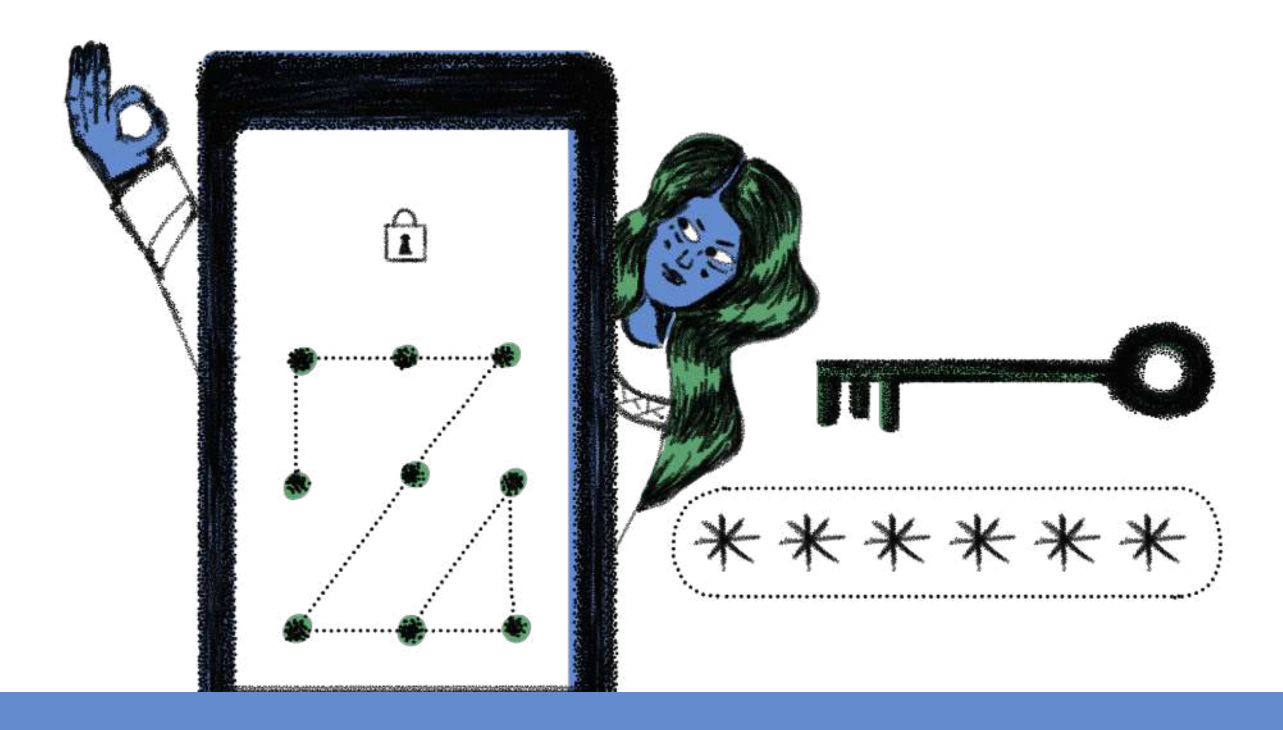
No obstante, **ello no está exento de dificultades, especialmente cuando existen limitaciones en la infraestructura tecnológica y barreras de acceso a internet.** Más aún, este último punto se presenta como un elemento determinante que influye en las posibilidades de las personas defensoras para aprovechar plenamente las tecnologías digitales en su labor diaria.

La creciente necesidad de tecnologías en la actualidad constituye un factor constante de vulnerabilidades y riesgos en seguridad digital para las personas defensoras de derechos humanos en Colombia. Las amenazas que enfrentan en el ciberespacio, como ataques a su privacidad y ciberacoso, y el uso indebido de sus datos, representan peligros significativos que pueden comprometer

tanto su seguridad personal como la de sus comunidades. Si bien el Estado ha implementado políticas para fortalecer la ciberseguridad y ciberdefensa a nivel nacional, estas no siempre se traducen en garantías concretas para los defensores que operan en entornos digitales. **De ahí la importancia de entender cómo estos riesgos digitales afectan a las personas defensoras, especialmente en contextos donde el acceso a recursos (como escenarios de formación y promoción) para mejorar la seguridad digital son limitados.**

La presente investigación se propone **analizar, a través de un enfoque mixto[1], las dinámicas de apropiación digital, acceso a internet, riesgos y seguridad digital entre las personas defensoras de derechos humanos en Colombia.** A partir de encuestas y grupos focales, se busca ofrecer un panorama exploratorio de las condiciones en que estas personas llevan a cabo su labor, las barreras que enfrentan para acceder y apropiarse de las tecnologías digitales, así como los riesgos específicos a los que están expuestos en el ámbito digital. Al combinar técnicas cuantitativas y cualitativas, este estudio pretende brindar información desde un primer punto de partida que ayuda a entender y aproximarse a las realidades diversas de los defensores, a fin de generar estrategias más efectivas para mejorar su seguridad y facilitar el acceso efectivo y contextualizado a la tecnología y a la digitalidad.

[1]Esta investigación tiene un enfoque mixto en tanto utiliza técnicas de estadística descriptiva para analizar la información obtenida de la encuesta a personas defensoras y análisis de información cualitativa recolectada a partir de entrevistas y grupos focales.



02. Marco teórico

A. Personas defensoras de derechos humanos

Un defensor o defensora de derechos humanos **es cualquier persona o grupo que se dedica a promover y proteger los derechos fundamentales reconocidos internacionalmente y nacionalmente.** Según la Defensoría del Pueblo de Colombia (2022) y el Alto Comisionado de las Naciones Unidas para los Derechos Humanos (s.f.), esta labor puede ser desempeñada por todo tipo de personas en diferentes contextos, ya sea en grandes organizaciones intergubernamentales, en sus comunidades locales, o incluso dentro del sector público o privado, lo esencial es su compromiso en la defensa de derechos humanos, sin importar su género, edad o profesión. En este sentido, las personas defensoras de derechos humanos están definidas por las acciones que llevan a cabo y su intencionalidad.

Además, la Corte Constitucional, en la Sentencia SU 546 de 2023, subraya que los conceptos de líderes sociales y defensores de derechos humanos son amplios y, en ocasiones, se utilizan indistintamente. Aunque un líder o lideresa social no se identifique como defensor, su trabajo en la promoción de derechos humanos le posiciona como tal.

La anterior definición asocia la defensa de derechos a todas las acciones que se lideran y se dan de forma pacífica, a través de diversas formas de liderazgo comunitario o social. Por ello, **en esta investigación se utiliza el concepto de persona defensora de derechos humanos indistintamente con el de líderes sociales,** en tanto todas las personas que participaron en el marco de las técnicas de recolección se identifican como actores que promueven de forma local los derechos de sus comunidades.

B.Apropiación digital

La apropiación digital se ha posicionado como uno de los principales objetivos de la política pública en Colombia (MinTic, 2010; MinTic, 2021)[2], pese a que hay poca

[2] Un estudio contratado por MinTic mide los logros de sus programas a partir de la clasificación de los promedios de los niveles de apropiación digital de sus beneficiarios como medida de éxito de todas las iniciativas vigentes para el año 2021: "Los programas que tienen los beneficiarios de mayores niveles de apropiación digital son los de Ciencia de Datos con 0,92 seguidos por Misión Tic Ruta 2 con 0,86. Los programas con niveles más bajos son: los de Formación de Personas con Discapacidad con 0,47, Usuarios Zonas Digitales Rurales 0,43 y Oferta Julio 2021 también con 0,43" (MinTic, 2021).

claridad en cuanto al concepto. Algunos indicadores lo han delimitado como la combinación entre el uso de aplicaciones y dispositivos conectados a internet con las intenciones de las personas al momento de realizar esos usos (Centro Nacional de Consultoría, 2023). No obstante, esta definición establece la apropiación digital como un proceso cuyo fin está centrado únicamente en la popularización y la divulgación social de estas herramientas, es decir, **se entienden los conocimientos tecnológicos y el uso de herramientas digitales como fines en sí mismos, y no como herramientas ligadas a otros objetivos** que van más allá de la expansión del uso de internet.

En este sentido, en el marco de esta investigación es importante separar la definición de apropiación digital de las ideas de popularización y divulgación del uso de internet (Franco Avellaneda y Pérez-Bustos, 2010), principalmente porque **la popularización y divulgación de internet está asociada a procesos macro que limitan la agencia de las personas en los mismos.**

Un ejemplo de ello es la instauración de trámites a través de internet, que implica que una agencia gubernamental traslade la prestación de un servicio al entorno digital, popularizando su uso, en un proceso en el que no hay participación de las personas usuarias directas en su diseño y traslado. Otro ejemplo esclarecedor es la popularización del consumo de contenido a través de redes sociales masivas como TikTok e Instagram, donde los algoritmos que escogen y comparten el contenido están diseñados lejos de la participación de las personas usuarias finales.

Por contraste, la apropiación digital **es un proceso social intencionado, liderado de forma conjunta por diferentes actores quienes se articulan con el objetivo de intercambiar, combinar, negociar y poner en diálogo conocimientos** (Franco Avellaneda y Pérez-Bustos, 2010). Esta definición involucra a las personas usuarias de las herramientas tecnológicas y digitales, en tanto que son ellas quienes, a partir de sus necesidades e intereses, buscan usar, aplicar, enriquecer, modificar, intervenir los conocimientos y las herramientas en un proceso constante de contextualización con sus realidades inmediatas.

Esta perspectiva reconoce a los actores sociales y comunitarios **como protagonistas de la apropiación digital, en lugar de simples receptores de información derivada de conocimientos expertos.** Esto no implica desconocer que existen actores en la producción y circulación de tecnologías con un papel predominante. Sin embargo, la apropiación está mediada localmente y de manera plural por los actores que buscan acercarse a estas herramientas. En este contexto, la apropiación digital se entiende y mide en función del proceso de adquisición, manipulación y uso de herramientas tecnológicas para promover la defensa de los derechos humanos.

C. Acceso a internet

El acceso a internet es una herramienta fundamental para interactuar con las tecnologías digitales, ya que permite el uso de diversas aplicaciones y herramientas. Debe comprenderse no solo desde una perspectiva técnica, sino también como un medio que facilita la comunicación, la integración en comunidades virtuales y la incorporación de la web en la vida cotidiana de las personas. Como plantea Grillo (2019), la web cobra sentido a través de los usos que las personas le otorgan.

Sin embargo, para Pérez de Acha (2018), **un acceso real va más allá de la simple conectividad, este involucra la capacidad de modificar las tecnologías, comprender su funcionamiento, integrarlas a la vida diaria y acceder a contenidos localmente relevantes.** Esta visión holística del acceso a internet incluye también la confianza en las tecnologías de la información y la comunicación (TIC), lo que resalta la importancia de un uso más profundo y significativo de la tecnología.

Por otro lado, Alva de la Selva (2015) destaca que el acceso a internet ha sido tradicionalmente visto como una cuestión de conectividad, es decir, de disponibilidad de equipos e infraestructura. No obstante, ella subraya que el **verdadero reto reside en la "barrera de los usos", es decir, en la capacidad individual de aprovechar las TIC de manera efectiva según las necesidades personales.** La superación de esta barrera es clave para asegurar una participación plena en la sociedad de la información.

En el marco de esta investigación, se retoma u**na definición de acceso a internet desde una perspectiva tradicional, enfocada en los dispositivos y la infraestructura que poseen las personas defensoras para utilizar herramientas digitales y conectarse a internet.** Esta definición permite medir de manera más clara y diferenciada el concepto de apropiación digital. Sin embargo, es importante destacar que no se pretende restar relevancia a las barreras relacionadas con la capacidad adquisitiva de las personas o sus habilidades para usar la tecnología digital de forma efectiva, entre otras. Aun así, es necesario delimitar el uso de este concepto en el análisis de los datos para entender su independencia frente a la definición propuesta de apropiación digital.

D.Seguridad digital

El Estado colombiano ha establecido una serie de lineamientos enfocados en la seguridad digital, que incluyen la protección de la infraestructura necesaria para la conexión y el almacenamiento de datos, así como la defensa del ciberespacio en el contexto de la protección de la soberanía nacional. Por su parte, el Manual de Políticas de Seguridad Digital del Ministerio de Educación Nacional (s.f.) hace hincapié en la protección de los activos informáticos y la información que circula en estos sistemas.

La seguridad digital abarca tanto aspectos técnicos, como las herramientas de seguridad informática, como también factores organizacionales, como las políticas y procedimientos que aseguran la integridad de los sistemas de información. El riesgo se entiende como la posibilidad de que una amenaza aproveche una vulnerabilidad, mientras que la vulnerabilidad se define como una debilidad en un sistema que puede ser usada para causar daño.

Por otro lado, el enfoque del CONPES 2020[3] sobre la seguridad digital está más orientado hacia **la defensa del Estado, concentrándose en la ciberseguridad y ciberdefensa a nivel estatal.** Se postula la creación de organismos como el ColCERT y el Comando Conjunto Cibernético con el objetivo de enfrentar amenazas cibernéticas que afectan la seguridad nacional. Este enfoque resalta la importancia de coordinar esfuerzos entre diferentes sectores del gobierno para mantener la estabilidad y defensa en el ciberespacio.

La comparación entre esas dos definiciones permite observar ambas facetas de la seguridad digital. Así, mientras que el Ministerio de Educación se enfoca en la seguridad digital desde una perspectiva más técnica y general (protección de activos informáticos y políticas de información), **el CONPES 2020 prioriza la ciberdefensa a nivel estatal, con un enfoque más estratégico y militarizado, destinado a contrarrestar amenazas a la seguridad nacional.** No obstante, este último documento empieza a generar una conceptualización sobre la seguridad y los riesgos digitales asociada con el uso de internet y de la tecnología por parte de la ciudadanía.

[3] En este documento se agregan apartados que buscan fortalecer la seguridad digital de la ciudadanía como uno de sus objetivos. No obstante, el desarrollo de herramientas como la apropiación digital de herramientas de seguridad por parte de comunidades, y de otros actores no estatales, no tiene el mismo desarrollo que la seguridad digital como herramienta de defensa del Estado.

03. Metodología

La investigación **se desarrolló utilizando un enfoque mixto, que combinó técnicas cuantitativas y cualitativas para obtener una visión integral** de la apropiación digital, los riesgos digitales, el acceso a internet y los incidentes de seguridad digital de las personas defensoras de derechos humanos en Colombia. En la fase cuantitativa, se aplicó una encuesta probabilística a 107 personas defensoras de derechos humanos en Colombia, seleccionadas a partir de la red de trabajo con organizaciones cercanas a la Fundación Karisma. La encuesta, conformada principalmente por preguntas cerradas, se diseñó para recopilar datos sobre su percepción de riesgos, acceso a protección y experiencias en su labor de defensa de derechos.

Además, se realizaron cinco grupos focales en diferentes regiones del país, con el objetivo de captar las experiencias más profundas y matizadas de las personas participantes. Estos grupos **se centraron en explorar temas como las dinámicas locales de violencia, las estrategias de defensa de derechos y los dispositivos y aplicaciones que utilizaban en su cotidianidad.** Las discusiones en estos grupos proporcionaron una visión cualitativa que complementa los hallazgos obtenidos a través de la encuesta, posibilitando sistematizar hallazgos emergentes con el fin de identificar variables no observables que no estaban contempladas en el diseño de la encuesta.

La combinación de estas dos metodologías permitió triangular de forma complementaria los datos y obtener una comprensión más amplia y detallada de la situación de las personas defensoras de derechos humanos en Colombia. Mientras que **la encuesta ofreció una visión más generalizable, los grupos focales brindaron un contexto y una profundidad adicionales a las estadísticas,** permitiendo interpretar mejor los resultados y generar recomendaciones adaptadas a las diversas realidades del país.

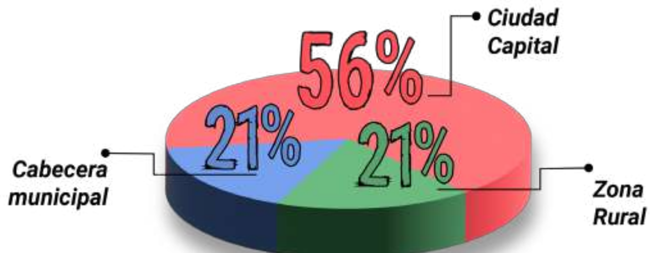


04. Descripción sociodemográfica de las personas encuestadas

El análisis de las características sociodemográficas de las personas encuestadas revela una mayoría en el rango de edad de 28 a 45 años (57,01 % de la muestra), mientras que el 25,23 % tiene entre 18 y 28 años, y solo el 0,93 % supera los 60 años. Esto indica que las **personas defensoras de derechos humanos en la muestra están mayormente concentradas en la edad productiva media, con poca representación de personas mayores**.

En cuanto a la educación, un 30,84 % posee un título profesional y un 26,17 % cuenta con estudios de posgrado, lo que indica un alto nivel educativo en esta población. **Solo un 0,93 % de las personas encuestadas tiene escolaridad primaria, lo que indica que la mayoría de los participantes ha alcanzado niveles avanzados de educación formal.** Los resultados que se exponen más adelante en este estudio pueden sugerir que el grado de escolaridad no necesariamente tiene una relación con los indicadores de apropiación digital, riesgos digitales y acceso a internet.

Geográficamente, el 44,86 % de las personas encuestadas reside en la Región Andina, mientras que el 32,71 % vive en la Orinoquía y el 21,50 % en la Amazonía; no existe representación de personas de las regiones pacífica y caribe. **Es importante destacar así que las personas encuestadas, que reportaron información en el marco de este estudio, no se encuentran en las zonas costeras de Colombia.**



Gráfica 1 (uno). Distribución de la zona de residencia

Finalmente, el 53,27 % de las personas encuestadas se identifica como mujer, y el 73,83 % se describe como heterosexual. Sin embargo, también se observa una participación relativamente alta de personas que reportaron identidades de género y orientaciones sexuales diversas, como mujeres trans (4,67 %) y hombres trans (3,74 %), así como un 14,02 % que se identifica como homosexual.

05. Hallazgos principales

A.Apropiación digital en personas defensoras de derechos humanos

Hallazgos principales en apropiación digital

1. La brecha en apropiación digital permite evidenciar que tres de cada cuatro personas defensoras cuentan con niveles medios y bajos de apropiación digital.

2. El 72 % de las personas entrevistadas no ha apropiado herramientas y/o aplicaciones digitales para avanzar en su agenda de incidencia.

3. Los objetos con los que menos cuentan las personas defensoras son disco duro externo, relojes inteligentes y asistentes de voz.

4. Las herramientas con las que menos cuentan y/o menos usan son cuentas de redes sociales exclusivas para el trabajo, transmisiones a través de redes sociales y software de seguridad.

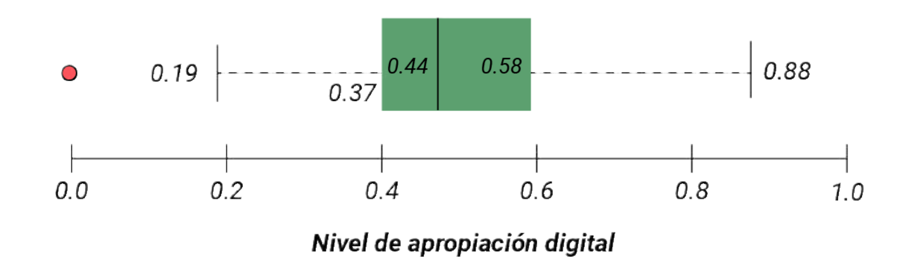
5. No hay diferencias significativas entre los diferentes rangos de edad en relación con sus niveles de apropiación digital.

6. La apropiación digital no es la variable más significativa al momento de explicar el aumento o la disminución de los riesgos digitales de las personas defensoras que reportaron información.

La construcción del indicador de apropiación digital estuvo basada en la información reportada por las personas defensoras de derechos humanos en la encuesta. Las preguntas que se utilizaron para construir este indicador fueron en torno a: (i) **su percepción de autosuficiencia** al momento de utilizar dispositivos y acceder a aplicaciones digitales, (ii) las actividades que realizan con la **conexión de internet,** (iii) **la cantidad de objetos** con los que cuentan para conectarse a internet, (iv) **las herramientas digitales utilizadas** en el marco de la defensa de los derechos humanos, y (v) si la persona **administraba cuentas de su organización.**

La construcción de este indicador se realizó ponderando cada uno de estos cinco componentes de forma individual. **Todas las respuestas tuvieron un valor equidistante de 1 al interior de la ponderación de cada componente, y a su vez cada componente tuvo el mismo valor en la ponderación del indicador global.** En este sentido, la metodología empleada para calcular el indicador de apropiación digital premió a las personas que administraban las cuentas de sus organizaciones. Por otro lado, se excluyeron algunos objetos en el marco de la ponderación del indicador, por ejemplo, el uso de botón de pánico, pues este elemento no es de uso cotidiano y solamente seis personas reportaron tenerlo[4].

Para presentar la información asociada al indicador de apropiación digital se utilizan gráficos boxplot. Un boxplot (o gráfica de cajas y bigotes) **es una gráfica que permite entender cómo están distribuidos los datos de un conjunto.** La caja representa el rango en el que se encuentran la mayoría de los datos, en tanto que la línea dentro de la caja muestra el promedio. Además, hay "bigotes" que salen, los cuales muestran hasta dónde llegan los valores más extremos. Finalmente, los puntos que salen de estas líneas representan casos atípicos de personas que tienen un comportamiento diferente.



Gráfica 2 (dos). Distribución en boxplot del indicador de apropiación digital

En la gráfica 2, donde 1 (uno) indica el máximo nivel de apropiación digital y 0 (cero) el mínimo, se puede observar que las personas defensoras están en un nivel de apropiación entre el 0,37 y el 0,58. Un 25 % de las personas tiene un rango superior a este intervalo, hasta alcanzar un máximo de 0,88. **¿Esto qué quiere decir?**

[4] Los botones de pánico son herramientas de protección que entrega la Unidad Nacional de Protección a personas defensoras de derechos humanos con el objetivo de alertar e informar en caso de ataques o riesgos.

El nivel de apropiación digital de las personas defensoras que reportaron información se encuentra en su mayoría en niveles bajos o medios. El 75 % de estas personas cuenta con pocos elementos de conexión, realiza actividades limitadas a través de internet, tiene un nivel bajo de autosuficiencia y pocas herramientas digitales en línea. También, hay un grupo pequeño de personas que tiene mayores niveles de apropiación digital.

Estas diferencias pueden estar determinadas por algunos elementos puntuales dentro del indicador. Por ejemplo, **solo el 28 % de las personas defensoras entrevistadas realizan actividades asociadas a la incidencia digital y a la promoción de los derechos humanos a través de herramientas digitales.** Es decir, pocas personas han apropiado, modificado, intervenido y contextualizado el uso de internet para llevar a cabo acciones de incidencia desde sus organizaciones.

Actividades que realizan en internet	% personas
Entretenimiento y comunicaciones (accede a redes sociales como Facebook, Twitter o TikTok, aplicaciones de mensajería como WhatsApp y servicios de streaming como Youtube, Spotify, Netflix)	77,57
Educación y trabajo (participa de reuniones virtuales para su trabajo o sus procesos de formación, publica noticias en plataformas propias como páginas web o blogs, recibe y comparte información por medios especializados)	78,50
Incidencia digital (desarrolla una agenda política o social a través de medios digitales, gestiona plataformas propias para la publicación de documentos o investigaciones en una área específica)	28,04

Tabla 1 (uno). Actividades realizadas por personas defensoras a través de herramientas digitales

Otro factor que podría explicar las diferencias en la distribución de este indicador está relacionado con los objetos de los que disponen las personas. Que una minoría posea ciertos objetos que no están al alcance de la mayoría podría estar vinculado a la capacidad económica para adquirirlos. En la siguiente tabla se presentan los objetos que fueron reportados en menor porcentaje por las personas encuestadas.

Elementos con los que cuentan las personas defensoras	% personas
Disco duro externo	10,28
Reloj inteligente o similares	12,15
Asistentes de voz (Alexa, Amazon Echo, Google Home, etc.)	7,48

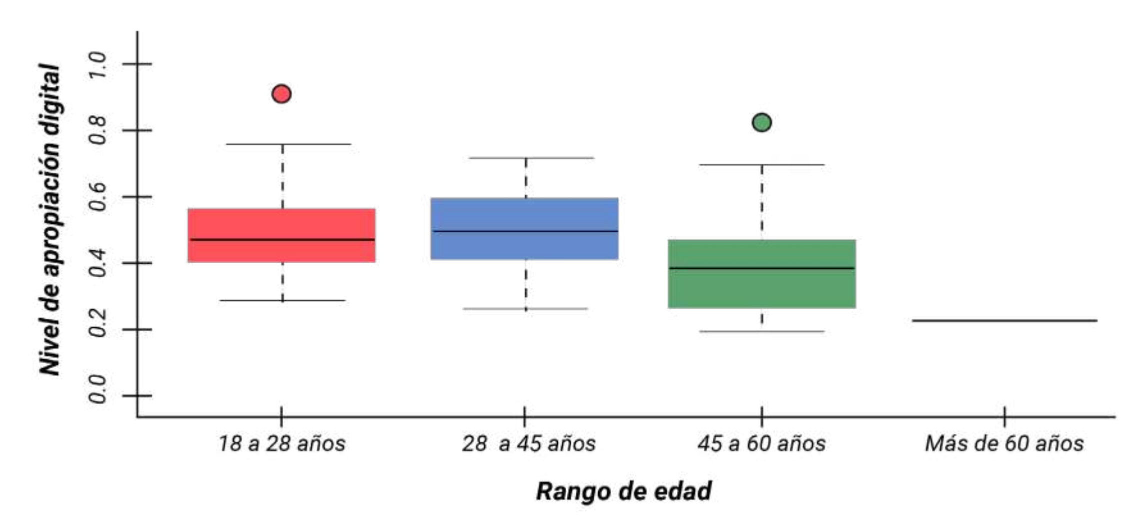
Tabla 2 (dos). Elementos con los que cuentan las personas defensoras

En cuanto a las herramientas digitales para la defensa de los derechos humanos, las que tienen menor uso son las cuentas exclusivas para el trabajo, las transmisiones en vivo y el software de seguridad. El bajo uso de estas herramientas puede ser uno de los factores que explica la distribución desigual del indicador de apropiación digital.

Herramientas digitales para el trabajo de defensa de los derechos humanos	% personas
Cuentas de redes sociales exclusivas para su trabajo (Twitter, Facebook, Instagram, YouTube, Snapchat, TikTok)	29,91
Transmisiones en vivo (Facebook Live, Instagram Live, Twitter Spaces, Twitch, Youtube en vivo, etc.)	8,41
Software de seguridad (antivirus, herramientas de elusión como VPN o TOR, de cifrado como PGP, Bitlocker, VeraCrypt, etc.)	13,08

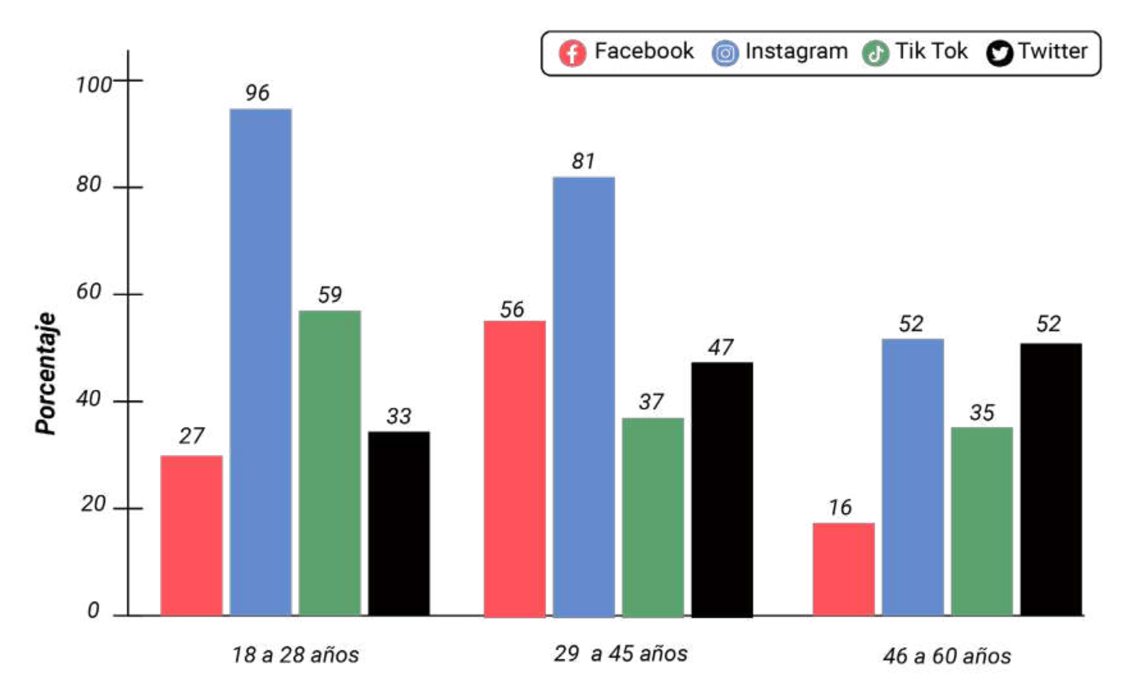
Tabla 3 (tres). Herramientas digitales para el trabajo de defensa de los derechos humanos

En cuanto a la distribución del indicador de acuerdo a los diferentes grupos poblacionales, se puede evidenciar que no hay diferencias marcadas entre todos los rangos de edad. Como se puede ver en la gráfica 3, casi la totalidad de los registros tiene una distribución similar del indicador. En consecuencia, **la edad no es un factor que aparentemente influya en los niveles de apropiación digital de esta población.**



Gráfica 3 (tres). Distribución en boxplot del indicador de apropiación digital por rango de edad

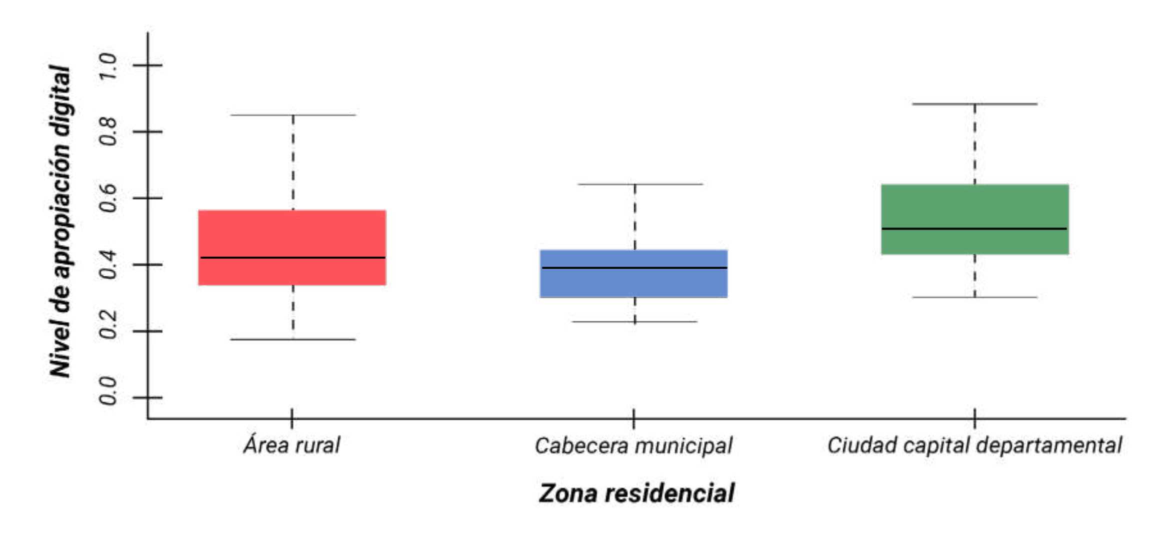
En relación con la edad, hay un contraste interesante en el uso de la red social Instagram, ya que el 96 % de las personas de 18 a 28 años la utiliza, así como también el 81 % de las personas entre 28 y 45 años, mientras que el 52 % de las personas entre 45 a 60 años no la usa. Esto muestra que **el uso de Instagram está concentrado en personas menores de 45 años,** por lo que puede ser una red más familiar para personas jóvenes. Como se puede ver en la gráfica 4, la distribución de uso de las demás redes sociales, a excepción de Twitter, mantiene esta tendencia.



Gráfica 4 (cuatro). Uso de redes sociales por edad

En cuanto a las aplicaciones de mensajería instantánea, todas tienen porcentajes similares en su uso a excepción de WhatsApp, para la que solo **2 (dos) personas reportaron que no la utilizan**. Esto significa que esta aplicación sigue siendo el sistema de mensajería instantánea que más uso ha adquirido en los últimos años; incluso se ha convertido en una red social para adquirir contactos y socializar con grupos más extensos.

En cuanto a la distribución con respecto al tipo de zona en donde viven las personas entrevistadas, la gráfica 5 muestra que quienes se encuentran en cabeceras municipales tienen menos niveles de apropiación digital en comparación con **las personas de otras zonas geográficas. Es decir que la zona donde viven las personas no parece tener incidencia en los niveles de apropiación digital.**

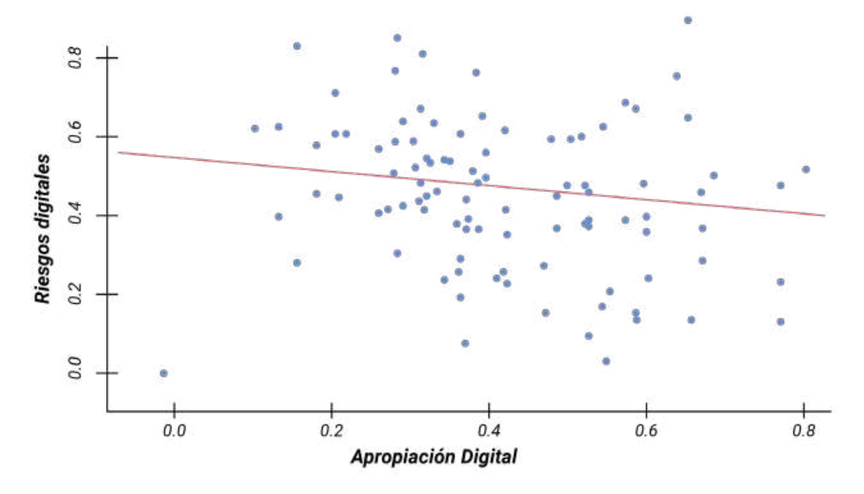


Gráfica 5 (cinco). Distribución en boxplot del indicador de apropiación digital por zona donde reside

Existe una relación inversa entre los niveles de riesgos digitales[5] y los niveles de apropiación digital. **¿Esto qué quiere decir?** Que entre más aumenta el indicador de apropiación digital de personas defensoras, más disminuye el indicador de riesgos digitales.

Esta relación podría sugerir que las personas que han apropiado a sus procesos de defensa más herramientas digitales y tecnológicas podrían tener menos riesgos asociados a la digitalidad, en tanto que toman mejores medidas de protección y cuidado. Sin embargo, el coeficiente de correlación[6] de estas variables es únicamente de -18 %, por lo que **la correlación realmente es muy débil, y hay muchos más factores que pueden explicar la disminución de los riesgos digitales.**

[5] En el apartado D se explica cómo se desarrolló el indicador de riesgos digitales a partir de la información auto reportada por las personas.
[6] Se realizó una prueba de correlación estadística basada en el coeficiente de Pearson.



Gráfica 6 (seis). Distribución del indicador de riesgos digitales en función del nivel de apropiación digital

B.Acceso a internet

Hallazgos principales en acceso a internet

1. Los niveles de acceso digital de las personas defensoras de derechos humanos son muy similares a lo largo de toda la muestra. A excepción de cuatro personas, quienes reportaron información de tener buenos niveles de acceso a internet.

2. Los puntos de conexión menos utilizados son los que generan más riesgos: café internet y puntos de conexión públicos.

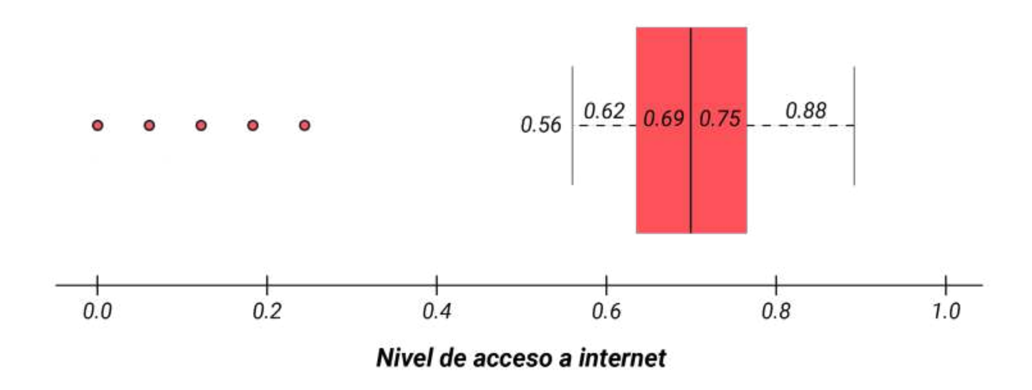
3. Al observar el comportamiento en áreas rurales, la desigualdad en acceso a internet es mayor. Esto no quiere decir que en estos lugares no se cuente con este servicio, sino que hay mucha desigualdad al interior de este grupo. Por lo tanto, en las zonas rurales hay un 25 % de personas con acceso a un internet similar al de zonas urbanas y cabeceras municipales, mientras que las demás se encuentran por debajo de esos niveles.

4. En las áreas rurales solo la mitad de las personas reportó tener un plan de datos personal, mientras que solo el 44 % reportó tener acceso a internet en casa y señal de teléfono. Esto puede explicar por qué hay más desigualdad en las zonas rurales con relación al acceso a internet.

5. No hay diferencias significativas en los niveles de acceso a internet entre hombres y mujeres dentro del estudio.

Este indicador particular estuvo basado en una comprensión tradicional del acceso que partió de ponderar las diversas formas que utilizan las personas defensoras para conectarse a internet. No se incluyó la utilización de dispositivos, en tanto que contar con estos dispositivos no implica poder acceder a conexión. En este sentido, se incluyeron variables que sí implican un acceso efectivo a internet, como son: (i) **los planes y puntos de conexión a los que tienen acceso efectivo** las personas defensoras, y (ii) el **autorreporte en torno a si cuentan o no con señal telefónica** en los lugares donde realizan su trabajo.

La construcción del indicador se realizó ponderando de forma individual cada uno de los puntos reportados, resultado que se contrastó con la respuesta en torno a si contaban o no con señal en los lugares donde realizaban sus trabajos. De estas manera, **el indicador premió a las personas que contaban con señal en contraposición a puntos de conexión individuales.**



Gráfica 7(siete). Distribución en boxplot del indicador de acceso a internet

En la gráfica 7, el 50 % de las personas que reportaron información de acceso a internet se encuentra entre los valores de 0,62 y 0,75. Al igual que con el indicador de apropiación digital, en este se puede observar que hay un 25 % de personas que tienen niveles más altos de acceso, en un rango entre 0,75 y 0,88, mientras que el otro 25 %, que cuenta con niveles de acceso menores, no se encuentra tan alejado de la mayoría, pues sus rangos oscilan entre 0,56 y 0,62. **¿Esto qué quiere decir?**

El nivel de acceso a internet de las personas defensoras de derechos humanos entrevistadas es muy similar a lo largo de toda la muestra. La gran mayoría se encuentra en un rango de 0,62 y 0,88, a excepción de cuatro personas que tienen niveles atípicos de bajo acceso. Esto quiere decir que la mayoría cuenta con acceso a internet, es decir, que las personas defensoras que reportaron información tienen la posibilidad de conectarse a la red. Es importante destacar que esto no implica una evaluación de la calidad de la conexión, sino de la diversidad de dispositivos y puntos de conexión.

Los modos de conexión menos utilizados que se reportaron fueron los planes de datos provistos por organizaciones, los café internet y el acceso a internet pública, siendo notorio que dos de estos modos son los menos seguros para conectarse a la red. En contraste, las modalidades que reportaron tener mayores usos fueron el plan de datos personal (78 %) y el internet en el hogar (71 %), lo que da cuenta de que **las personas defensoras que reportaron información cuentan con puntos de conexión constantes y cercanos para acceder a internet.**

Formas de conexión a internet	% personas
Plan de datos provisto por una organización de cooperación internacional	8,41
Café internet	2,80
Internet pública (bibliotecas, puntos Vive Digital, parques, pines, etc.)	14,95

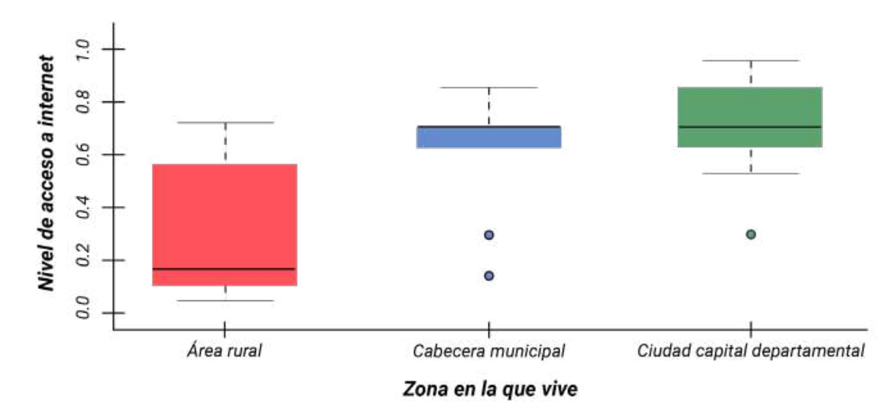
Tabla 4 (cuatro). Puntos de conexión a internet de las personas defensoras

En contraste, cuando se observa la distribución del acceso a internet, según las zonas de residencia, se puede deducir que hay una caída en el indicador referido a las zonas rurales. Esto señala que **las personas defensoras que viven en zonas rurales tienen menos puntos de conexión a internet y una señal celular mucho más débil en los lugares en donde realizan sus acciones de trabajo.**

Señal de teléfono por zona donde vive	% de quienes no cuentan con buena señal	% de quienes cuentan con buena señal
Área rural	55	44
Cabecera municipal	9	90
Ciudad capital	7	93

Tabla 5 (cinco). Señal de teléfono por zona donde vive

Como se mencionó al inicio, al ponderar las respuestas, la señal de celular es el factor que tiene mayor peso dentro del indicador. En la tabla 5 se puede observar que este elemento explica por qué **las personas defensoras encuestadas que trabajan en zonas rurales presentan una distribución con niveles más bajos en relación con el indicador de acceso a internet.**



Gráfica 8 (ocho). Distribución en boxplot de acceso a internet por las zonas de residencia

Como se puede observar, la gráfica 8 indica más desigualdad en las zonas rurales con respecto a los niveles de acceso a internet. Si bien, **el 25 % de las personas con mayores niveles de acceso a internet en estas zonas está en los mismos rangos que la mayoría de las personas de cabeceras municipales y de ciudades departamentales,** hay un 75 % restante que se encuentra fuera de este rango. En este mismo sentido, la distribución más grande es la de las zonas rurales, lo que da cuenta de cómo en estas zonas hay diferencias muy marcadas en acceso a internet. Esto se hace más explícito al observar de forma detallada los porcentajes de los puntos de acceso más constantes, como se puede ver en las tablas 6 y 7.

Señal de teléfono por zona donde vive	% de quienes no cuentan con buena señal	% de quienes cuentan con buena señal
Área rural	50	50
Cabecera municipal	19	80
Ciudad capital	13	86

Tabla 6 (seis). Plan de datos personal distribuido por zonas de residencia

Señal de teléfono por zona donde vive	% de quienes no cuentan con buena señal	% de quienes cuentan con buena señal
Área rural	55	44
Cabecera municipal	23	76
Ciudad capital	22	77

Tabla 7 (siete). Internet en el hogar distribuido por zonas de residencia

Como se puede observar, la gráfica 8 indica más desigualdad en las zonas rurales En las dos tablas se puede observar que hay una diferencia marcada entre los porcentajes de personas con acceso a internet en el hogar y plan de datos, según las zonas de residencia. Esto no implica que entre las personas que reportaron información, que se encuentran en zonas rurales, no se cuente con estos servicios, sino que **en este grupo hay mayor desigualdad a lo largo de toda la muestra.**

C.Riesgos de seguridad digital

Hallazgos principales de riesgos de seguridad digital

1. La amplitud en la distribución del indicador de riesgos digitales entre el 25 % menos expuesto y el 25 % más expuesto da cuenta de la amplia desigualdad que hay en el marco de la exposición de riesgos.

2. Las medidas de protección menos utilizadas son aquellas que van dirigidas al cuidado de las redes y los puntos de conexión wifi.

3. Las medidas de protección de cuidado de la información menos utilizadas no requieren de formación técnica y/o uso de aplicaciones sofisticadas, sino que están asociadas a cambios en los hábitos de uso y apropiación de tecnologías digitales.

4. La medida de protección de los dispositivos más usada es el uso de las contraseñas; sin embargo, hay un contraste con el uso de antivirus, principalmente en los celulares de las personas defensoras.

5. La disminución en los riesgos digitales no está causada únicamente por los niveles de apropiación digital. Hay muchos otros factores que deben investigarse y tomarse en cuenta al momento de fomentar prácticas de seguridad digital.

6. El nivel de acceso a internet no aumenta ni disminuye los niveles de riesgos digitales a los que se enfrentan las personas defensoras. No importa qué tan escaso o lejano se reporte el acceso a internet, este no afecta el nivel en que una persona está expuesta a sufrir amenazas y vulneraciones.

El indicador de riesgos digitales no se basa en la evaluación de las vulnerabilidades de las personas defensoras de derechos humanos, ya que no es posible realizar una evaluación objetiva de los riesgos en sus dispositivos. Tampoco se fundamenta en la medición de incidentes digitales, pues únicamente se dispone de los autorreportes de las personas defensoras. La construcción del indicador se basó en **el reporte de las medidas de seguridad que estas personas toman para proteger sus dispositivos, su información y sus redes de conexión.**

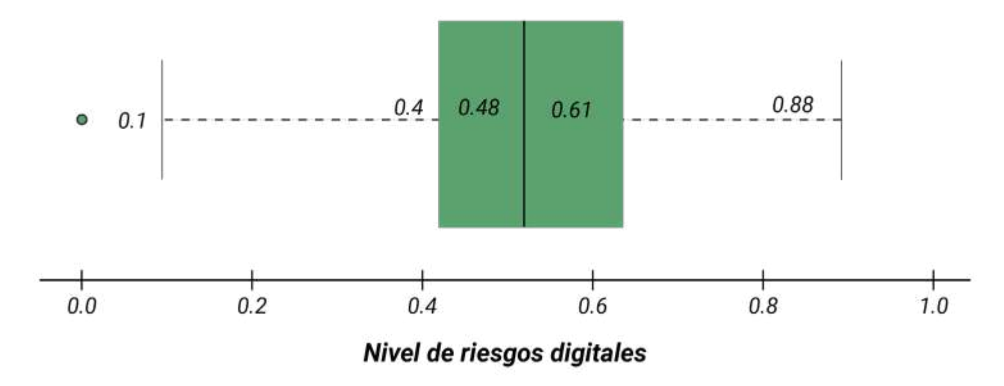
Con base en la aplicación de la encuesta, este indicador se construyó a partir de: (i) el uso o no de **medidas de seguridad para cuidar las contraseñas** de las cuentas, (ii) la constatación de que **se comparten los dispositivos con terceras personas**, (iii) el **uso de dispositivos de terceras personas** por parte de las personas defensoras, (iv) las medidas utilizadas para **proteger los dispositivos** de cada una de las personas defensoras, (v) las medidas utilizadas para **proteger el almacenamiento** de información, (vi) las medidas utilizadas para **proteger los puntos de conexión wifi,** y (vii) la percepción individual de de **la ocurrencia de amenazas digitales.**

El indicador se construyó ponderando cada uno de estos componentes de forma individual, con un enfoque en los riesgos digitales. Así, los elementos reportados como riesgos sumaban en la ponderación, al igual que cuando las personas indicaban no realizar las medidas de protección consultadas. Dos ejemplos ilustran mejor cómo se llevó a cabo este proceso:

Caso 1 (uno): cuando una persona reportaba utilizar la misma contraseña para más de una de sus cuentas, esto sumaba al indicador de riesgos.

Caso 2 (dos): cuando una persona no reportaba tener copias de respaldo para su información, esto sumaba al indicador de riesgos digitales.

En este sentido, el indicador mide **qué tan expuestas se encuentran las personas defensoras de derechos humanos** a sufrir un incidente de seguridad digital que afecte sus dispositivos, su información, sus cuentas y/o sus puntos de conexión de internet. Es importante hacer énfasis en que este indicador se construyó a partir de la información autorreportada por las personas, y no hace parte de un ejercicio de revisión y contrastación con los dispositivos usados.



Gráfica 9 (nueve). Distribución en boxplot del indicador de riesgos digitales

En la gráfica 9, se puede observar que el 50 % de las personas tiene un nivel de riesgos digitales entre 0,4 y 0,61. La distribución también muestra que el 25 % de quienes tienen más riesgos y el 25 % de quienes tienen menos riesgos están mucho más dispersos que el 50 % de personas que se encuentran en el medio. **¿Esto qué quiere decir?**

Los niveles de riesgo muestran una gran desigualdad entre las personas con mayores y menores niveles de exposición a riesgos digitales. Es decir, mientras algunas personas están muy poco expuestas, otras están altamente expuestas. Esto sugiere una notable desigualdad en cuanto a la formación y conocimientos sobre el cuidado y la protección frente a riesgos digitales entre quienes reportaron información.

En cuanto al cuidado de dispositivos, **la dispersión se puede explicar por el poco uso de antivirus en dispositivos como celulares.** En la tabla 8 se puede observar que, si bien el 88 % de las personas cuenta con claves para acceder a sus celulares, solamente el 15 % de estas personas utiliza antivirus en estos dispositivos. En general, este comportamiento resulta similar para los diferentes grupos poblacionales, dado que todas las personas utilizan o no las mismas medidas de seguridad para proteger sus dispositivos.

Medidas de seguridad utilizadas para cuidar dispositivos	% personas
Tengo clave de acceso (contraseña, pin, patrón o huella) en el teléfono	88,79
Uso antivirus en mi celular	15,89

Tabla 8 (ocho). Medidas de protección de dispositivos

En cuanto al cuidado de la información, las medidas menos utilizadas son el cifrado de datos, el almacenamiento seguro de contraseñas, la revisión de configuraciones y la realización de copias de respaldo. **Estas prácticas podrían estar asociadas con el 25% de personas que reportaron los menores niveles de riesgo digital,** ya que al realizarlas, se diferencian de la tendencia general del indicador. Es importante destacar que muchas de estas medidas no requieren habilidades técnicas ni aplicaciones nuevas para implementarse, sino que dependen de hábitos que pueden adquirirse en el proceso de uso y apropiación de las tecnologías.

Medidas de seguridad utilizadas para cuidar información	% personas
Almacenar las contraseñas en un lugar seguro o en un programa de gestión de contraseñas (KeePass, 1Password, etc.)	10,28
Cifrar el contenido de mis dispositivos	3,74
Revisar regularmente las configuraciones de seguridad y privacidad de mis cuentas y dispositivos	17,76
Hacer copias de respaldo en soportes externos como discos duros externos y memorias USB	12,15

Tabla 9 (nueve). Medidas de protección de la información

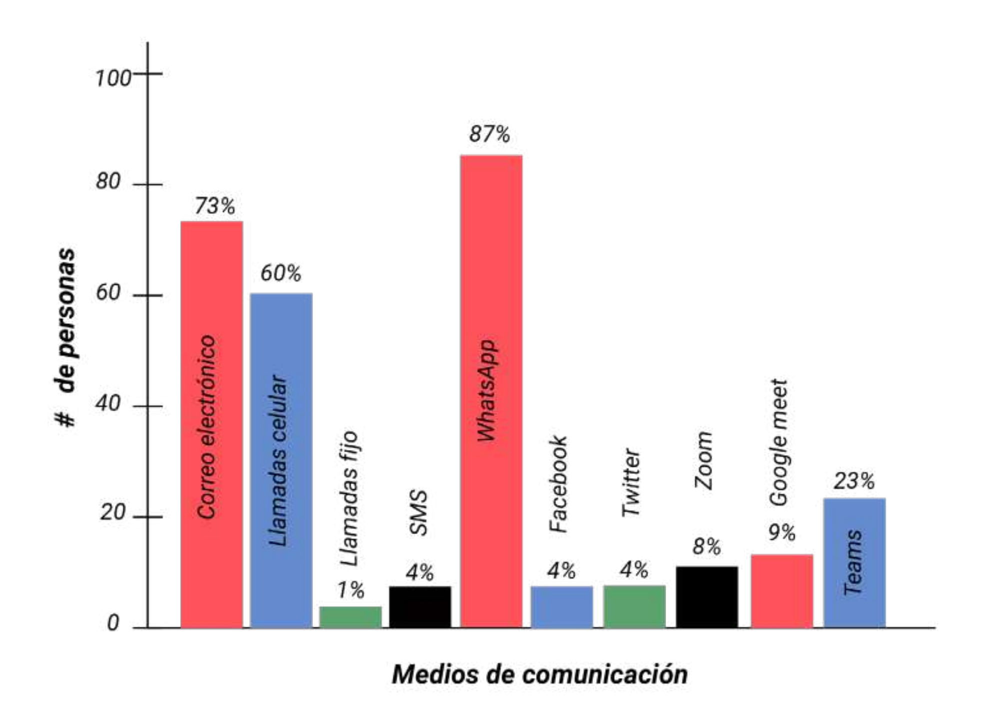
Las medidas de cuidado para proteger los puntos de conexión a wifi son las menos utilizadas. Si bien el **70% de las personas utiliza contraseñas para proteger sus redes de wifi, todas las otras medidas que se preguntan no son utilizadas.** El uso de estas medidas puede estar asociado igualmente al 25 % de personas con menores niveles de riesgo; no obstante, dentro de ese 25 % hay una variedad muy amplia.

Medidas de seguridad utilizadas para cuidar la conexión wifi	% personas
Cambia la contraseña de la red wifi periódicamente	25,23
Existe una red para invitados diferente a la red de uso propio	4,67

Tabla 10 (diez). Medidas de protección de los puntos de conexión

Si bien muchas de estas medidas pueden ser fortalecidas a partir de cambios en los hábitos del uso y apropiación de las tecnologías, s**olamente una de cada cuatro personas encuestadas ha recibido capacitaciones asociadas a temas de seguridad digital.** En esta misma vía, solamente el 15 % ha recibido algún tipo de análisis de riesgos digitales en el marco de sus trabajos. Finalmente, solo el 18 % de las personas defensoras que reportaron información se encuentran en organizaciones que cuentan con protocolos para el registro de incidentes digitales.

En uno de los grupos focales realizados en la región de la Amazonía, WhatsApp fue descrita como la herramienta predominante, utilizada para diversos propósitos, desde la comunicación personal hasta la coordinación de actividades laborales y la denuncia de situaciones críticas (grupo focal 3 (tres), 2024). Esta preferencia se confirma en la encuesta, donde el 87 % de las personas indicó que WhatsApp es su medio de comunicación más utilizado, seguido del correo electrónico (73 %) y las llamadas de celular (60 %). Esta diferencia es significativa en comparación con el uso de otras aplicaciones.



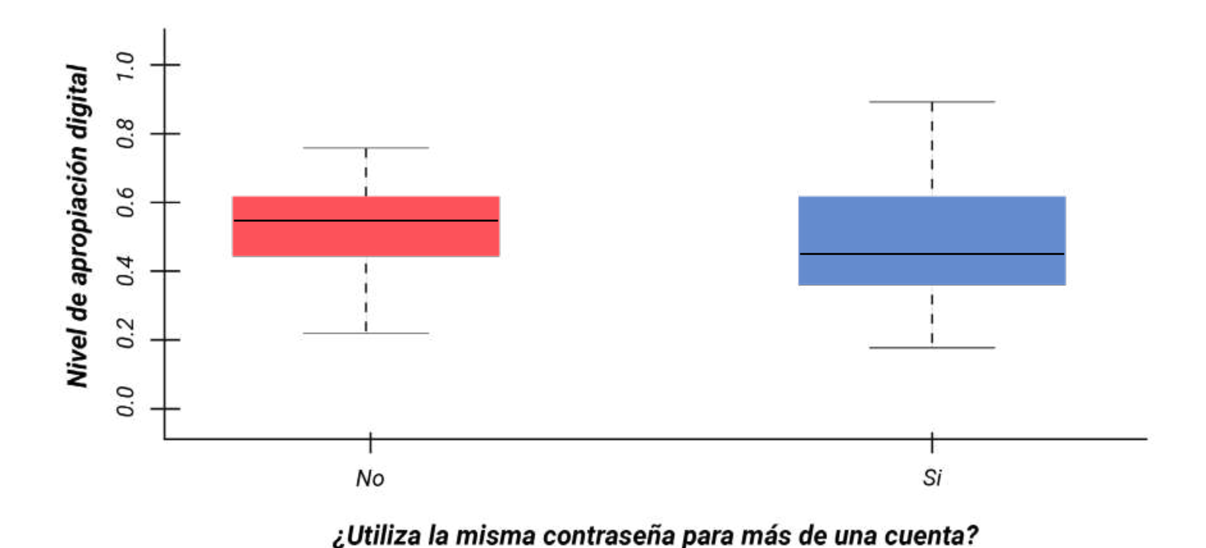
Gráfica 10 (diez). Porcentajes de medios de comunicación utilizados

Esta tendencia se mantiene no solamente en las diferentes zonas donde viven las personas defensoras, sino también en los rangos etarios en los que se encuentran. No obstante, y en contraste, en uno de los grupos focales se menciona que **el uso de llamadas y mensajes de texto se da en lugares de baja conexión,** mencionándose en el espacio que "dado que en algunas áreas la conectividad puede ser inestable, incluso llegando a durar días sin acceso a internet, los participantes recurren a métodos más tradicionales como llamadas y mensajes de texto" (grupo focal 2 (dos), 2024).

En cuanto al correo electrónico, en los grupos focales se explicó que su uso recurrente se debe a que se percibe como un canal esencial para enviar información importante y realizar denuncias (grupo focal 3 (tres), 2024). Sin embargo, el uso de estas aplicaciones puede implicar riesgos al compartir información y datos, ya que las llamadas y correos no están cifrados y pueden ser vulnerables a ataques.

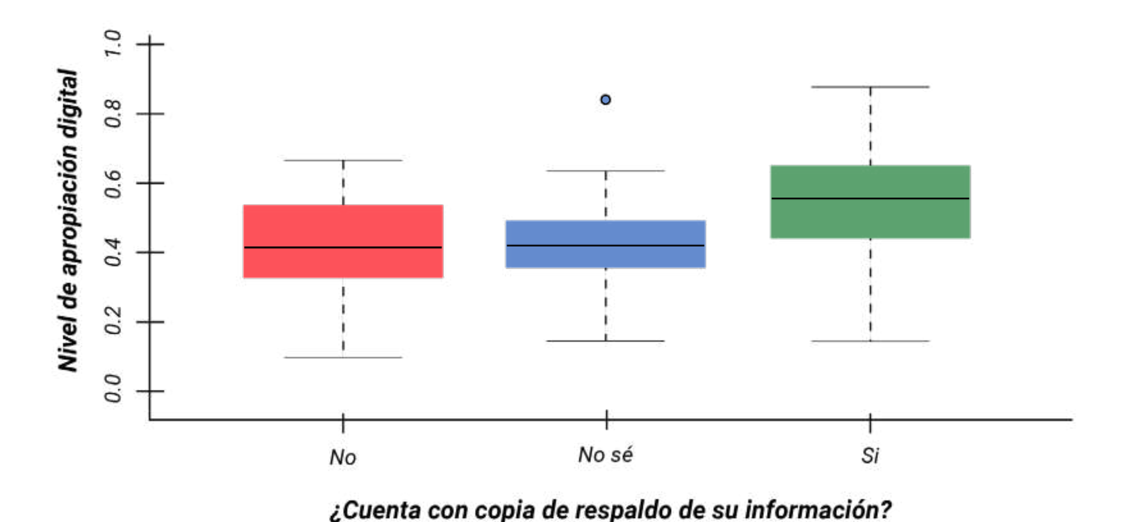
En cuanto a WhatsApp, los riesgos pueden estar relacionados **principalmente con aplicaciones paralelas no oficiales, como WhatsApp Plus,** además de que el uso de esta aplicación de forma combinada para relaciones personales y laborales puede llevar a compartir información personal de las personas defensoras (grupo focal 4 (cuatro), 2024) y a la ausencia de privacidad adecuada. Pese a ello, una característica positiva de WhatsApp es que su información se encuentra cifrada de extremo a extremo.

Los niveles de apropiación digital, como se mencionó en el primer apartado, no son el único factor que explica la disminución de los riesgos digitales. La distribución del indicador de apropiación digital asociado a la utilización de la misma contraseña para más de una cuenta puede ejemplificar esto. Como se ve en la gráfica 11, esta distribución no tiene cambios significativos cuando se compara entre quienes sí utilizan la misma contraseña y quienes no lo hacen, lo cual refuerza la idea de que **la apropiación no es la variable que mejor explica la disminución de riesgos digitales.**



Gráfica 11. Distribución de apropiación digital por uso de la misma contraseña

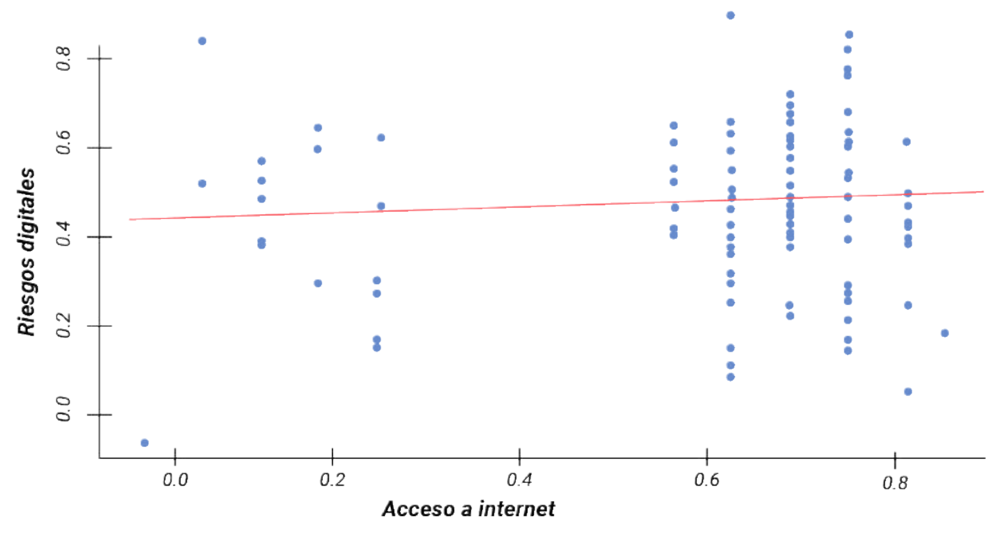
En esta misma vía, se puede observar en la gráfica 12 que la distribución del indicador de apropiación digital entre las personas que realizan y las que no realizan copias de seguridad de información no tiene diferencias significativas entre sí. En este sentido, la modificación de los hábitos de seguridad no está asociada con la experticia de las personas al manejar o utilizar los dispositivos y las aplicaciones digitales, sino **que debe estar asociado al fomento intencionado de prácticas de seguridad** con respecto a la información, los dispositivos, la comunicación y los puntos de conexión.



Gráfica 12. Distribución de apropiación digital por copia de respaldo de la información

Finalmente, la relación entre los riesgos digitales y el acceso a internet es positiva, aunque extremadamente débil, por lo que se puede asumir que no hay relación alguna, como se puede ver en la gráfica 12. **¿Esto qué quiere decir?** La tendencia entre las personas defensoras que reportaron información sugiere que a medida que aumenta su acceso a internet, más aumentan sus riesgos digitales. Sin embargo, el coeficiente de correlación[7] es únicamente del 6 %, muy cercano a 0 (cero), por lo que se puede afirmar que, para estas personas, su acceso a internet no tiene relación con sus niveles de riesgos digitales. En términos prácticos, esto significa que, sin importar qué tan lejana o escasa sea la conexión a internet de una persona defensora, su nivel de riesgo puede seguir siendo alto.

[7] Se realizó una prueba de correlación estadística basada en el coeficiente de Pearson.



Gráfica 13. Distribución de los riesgos digitales en función de los niveles de acceso a internet

D.Incidentes de seguridad digital y violencia a través de medios digitales

Hallazgos principales de riesgos de seguridad digital

1. Los incidentes más reportados fueron el ingreso no autorizado a dispositivos, el phishing con el objetivo de robar información y la suplantación y la alteración de la información.

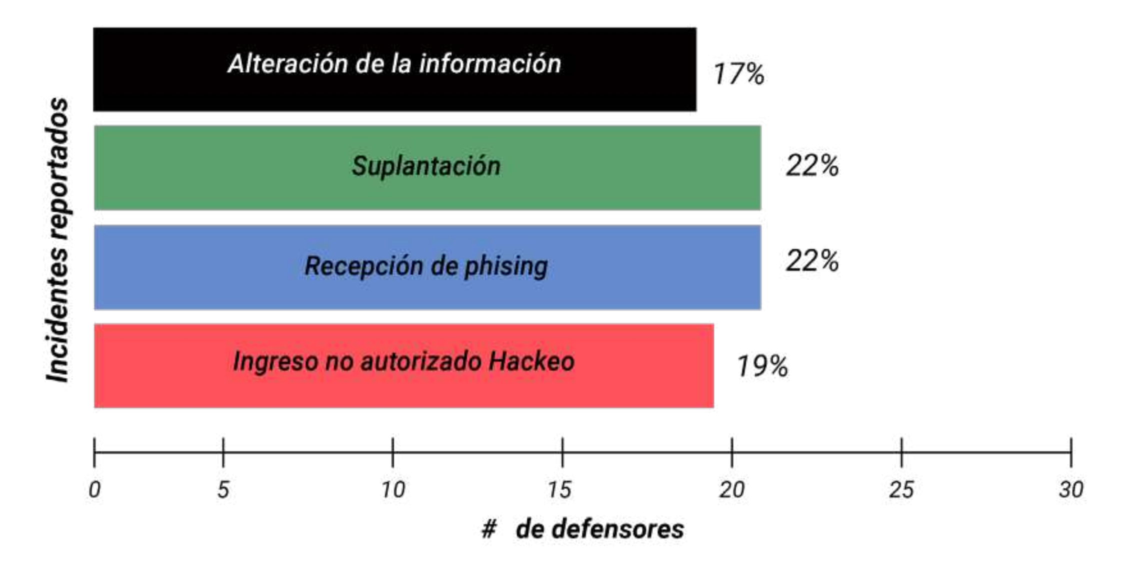
2. No existe un consenso entre las personas defensoras sobre cuál es la ruta más común para denunciar estos incidentes.

3. De las personas defensoras que reportaron información, quienes implementan más medidas de protección para su información, dispositivos y puntos de conexión no necesariamente experimentan menos incidentes digitales.

4. Las personas defensoras que reportaron información comparten una preocupación generalizada por la vigilancia, lo que genera desconfianza en la seguridad de las comunicaciones. Este es un temor asociado con escenarios de conflictividad.

Los incidentes en seguridad digital hacen referencia a los riesgos que se materializan a partir de una vulnerabilidad de información, de los dispositivos, o de los puntos de conexión. En el marco de este ejercicio de investigación, se asumen los reportes de ocurrencia de incidentes de seguridad digital reportados por las personas entrevistadas. No se realizó ningún ejercicio de contrastación para reafirmar o negar la ocurrencia de estos hechos.

Tales situaciones son acciones que afectan tanto el ámbito familiar como de trabajo de las personas defensoras. No obstante, estas acciones están encaminadas de forma directa a afectar las agendas de defensa de derechos lideradas de forma local por las personas líderes y por sus organizaciones. Como se puede observar en la gráfica 14, **los incidentes que más reportaron las personas fueron el ingreso no autorizado a sus dispositivos, el phishing con el objetivo de robar información, la suplantación y la alteración de la información.**



Gráfica 14. Incidentes de seguridad digital más reportados por las personas defensoras

A pesar de que ninguno de estos incidentes supera el 22 %, **el 50 % de las personas encuestadas reportó haber recibido amenazas a través de medios digitales.** Esta es una de las afectaciones más sufridas por las personas defensoras en el marco del uso y apropiación de medios digitales. Si bien este incidente no necesariamente está asociado a la información, a los dispositivos o a los puntos de conexión, da cuenta de la forma en que se pueden ampliar las dinámicas de persecución y seguimiento a las personas defensoras a través de la digitalidad.

En contraste, en la tabla 11 se pueden observar los incidentes de seguridad menos sufridos por las personas defensoras de derechos humanos. En esta lista **se encuentra el borrado y el secuestro de la información en sitio web, junto con la confiscación de dispositivos por parte de las autoridades,** afectaciones que fueron informadas por cuatro de las personas entrevistadas.

En el marco de uno de los grupos focales realizados en la región de la Amazonía, algunos participantes manifestaron que sus celulares son frecuentemente confiscados por grupos armados a través de retenes. Siguiendo con el testimonio de las personas defensoras en el espacio, **la confiscación no solo implica la pérdida temporal de los dispositivos, sino que también está asociada a la revisión de contenido personal y profesional,** lo que pone en riesgo la información sensible almacenada en los teléfonos (grupo focal 3 (tres), 2024). Por ello, si bien este tipo de incidentes no fue altamente reportado, sí es uno de los que implica mayor riesgo para la vida de las personas defensoras.

Incidentes de seguridad digital menos reportados por las personas defensoras	% de personas
Secuestro de información de la organización con fines extorsivos (ransomware)	3,74
Borrado de información en el sitio web de la organización o plataformas de terceros donde se almacena información	3,74
Alteración de la información en el sitio web de la organización o plataformas de terceros donde se almacena información	3,74
Confiscación de dispositivos por autoridades (Policía, Ejército, Fiscalía)	3,74

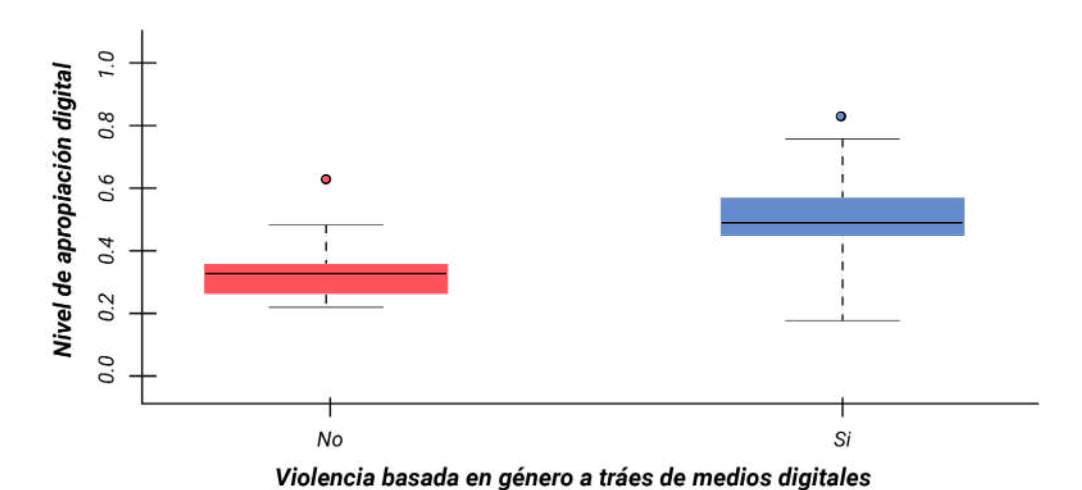
Tabla 11. Incidentes reportados por personas defensoras

En cuanto a la violencia basada en género sufrida por las personas entrevistadas, **se puede observar que los hombres reportaron sufrir muchos menos incidentes de este tipo en comparación con las mujeres**, y otras identidades de género.

Reporte de violencias basadas en género	No	Si
Hombre	91,6 %	8,3 %
Hombre trans	50 %	50%
Mujer	54,4%	45,6%
Mujer trans	0	100%
No quiero compartir esa información	0	100%
Persona no binaria	0	100%

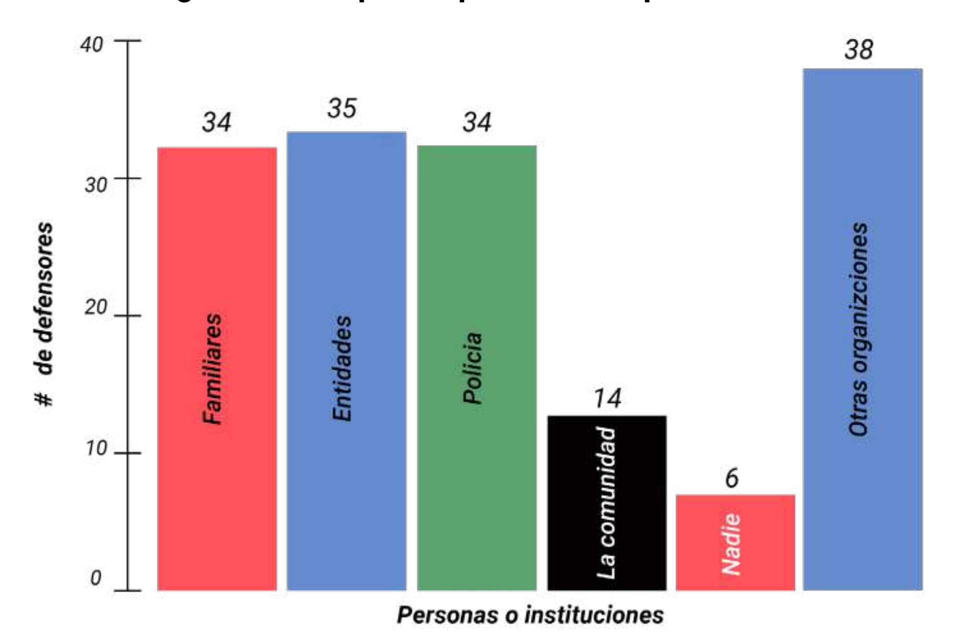
Tabla 12. Violencia basada en género por identidad de género

Las formas de violencia de género más reportadas en el ámbito digital fueron el ciberacoso (14 %), la ofensa sexual (16 %), la discriminación (14 %) y el acoso sexual (14 %). Es posible que estos casos estén subregistrados incluso entre las personas encuestadas, ya que al observar los niveles de apropiación digital de quienes reportaron violencias basadas en género, se evidencia que estas personas presentan mayores niveles de apropiación digital. Esto podría indicar que quienes no reportaron estas violencias podrían no reconocerlas como tales.



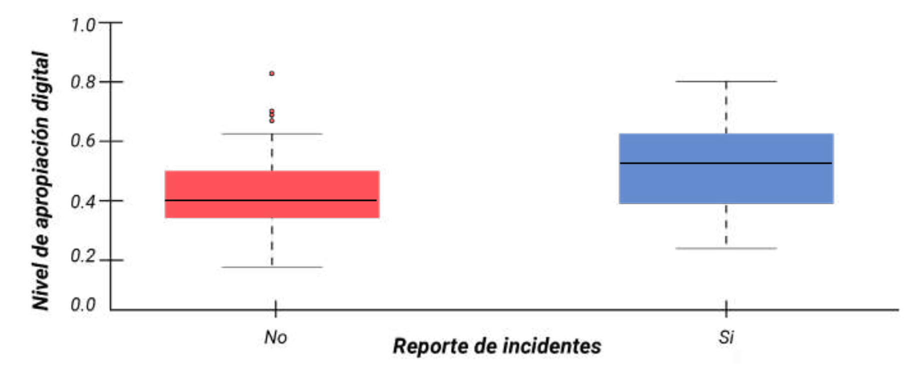
Gráfica 15. Reporte de violencia de género digital por nivel de apropiación digital

En cuanto a los lugares a los que las personas encuestadas acudirían para reportar casos y buscar ayuda en situaciones de incidentes de seguridad digital, la mayoría menciona otras organizaciones, seguidas por entidades gubernamentales, familiares y la policía. Estos datos revelan que **no existe un consenso entre las personas defensoras sobre cuál es la ruta más común para denunciar estos incidentes. No obstante, es importante destacar que solo seis personas indicaron que no tomarían ninguna acción para reportar este tipo de incidentes.**



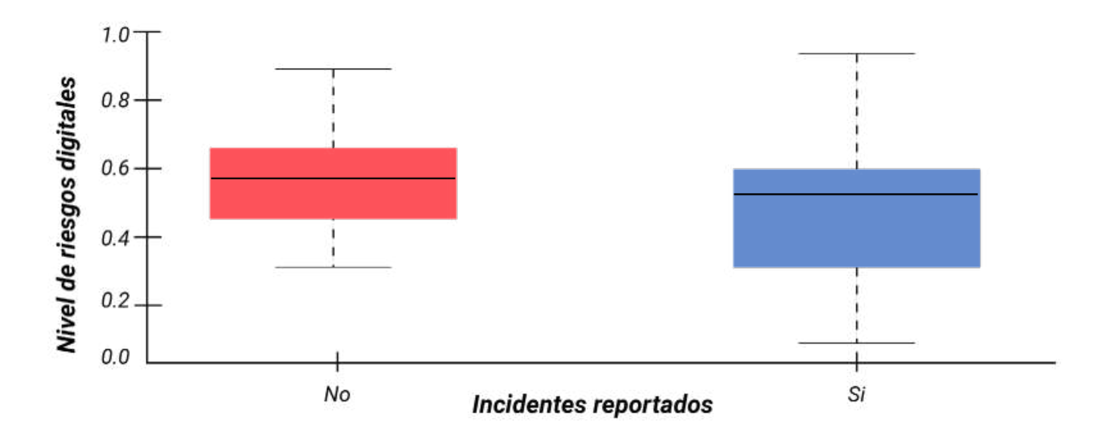
Gráfica 16. Instituciones o personas a las que acudiría para reportar incidentes de seguridad digital

En la misma vía de lo que sucede con las violencias basadas en género en escenarios digitales, se puede observar que hay una diferencia marcada en la distribución del indicador de apropiación digital entre quienes sí reportan incidentes de seguridad y quienes no lo hacen. Esto puede significar que en estos casos haya también un subregistro, **porque las personas con mayores niveles de apropiación digital podrían identificar de forma más clara este tipo de incidentes.**



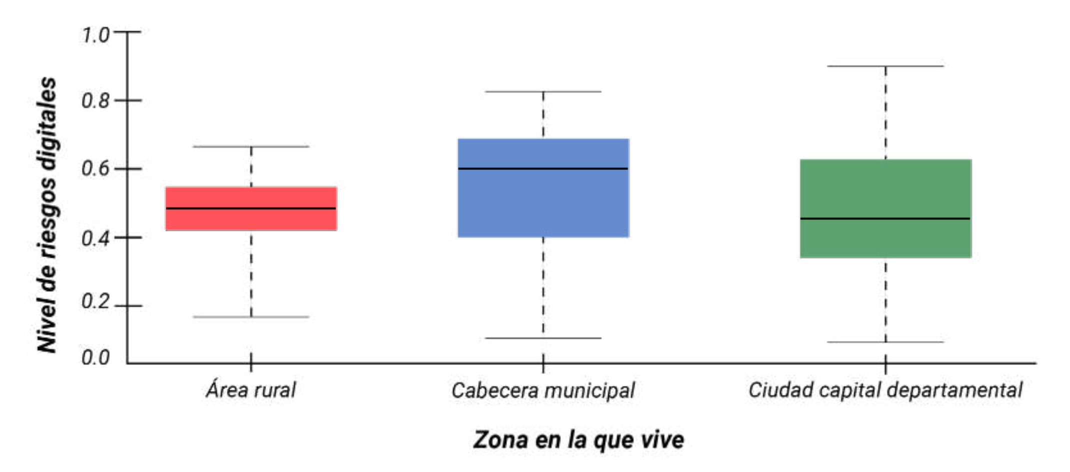
Gráfica 17. Nivel de apropiación digital por reporte de incidentes de seguridad digital

En cuanto a la distribución del indicador de riesgos digitales entre las personas que reportaron no haber sufrido incidentes, en la gráfica 18 se puede observar que no hay una diferencia marcada entre ambos grupos. Esto quiere decir que, entre las personas que reportaron información, **aquellas que utilizan más medidas de protección para su información, sus dispositivos y sus puntos de conexión no necesariamente sufren menos incidentes digitales.**



Gráfica 18. Nivel de apropiación digital por reporte de incidentes de seguridad digital

En cuanto a la distribución de los riesgos de seguridad entre los diferentes grupos poblacionales, se puede observar que no hay una diferencia marcada entre las tres áreas geográficas. Es decir, **la exposición a este tipo de vulnerabilidades no necesariamente se asocia al lugar específico donde viven las personas,** ni tampoco con los niveles de acceso que se vieron anteriormente.



Gráfica 19. Nivel de apropiación digital por reporte de incidentes de seguridad digital

En cuanto a los testimonios compartidos en los grupos focales, el primero, realizado en la región de la Orinoquía con personas defensoras que se desplazan entre zonas rurales y cabeceras municipales, sugiere que **el uso de versiones no oficiales de aplicaciones, como WhatsApp Plus[8], representa un riesgo significativo para la seguridad de la información, dado que no cuentan con las mismas protecciones que las versiones oficiales.** A pesar de la popularidad de estas herramientas, muchas personas desconocen cómo configurar adecuadamente la privacidad y seguridad, lo que subraya la necesidad de promover la sensibilización en este aspecto.

Aunque algunas de estas personas utilizan herramientas como VPN y Signal para asegurar las comunicaciones laborales, persisten riesgos debido a la falta de prácticas consistentes de seguridad. Además, **existe una preocupación generalizada por la vigilancia, lo que genera desconfianza en la seguridad de las comunicaciones, un temor que está asociado con escenarios de conflictividad.** Otro problema proviene del uso de contraseñas inseguras, ya que la mayoría de las personas reutiliza la misma contraseña en múltiples cuentas, lo que compromete gravemente la protección de sus datos.

En esta misma vía, con el grupo focal 2 (dos), se pudo observar que algunas de **las personas no contaban con contraseñas para proteger sus dispositivos, y en muchos de los casos, estas contraseñas eran débiles o almacenadas de forma poco confiable**. Asimismo, en el grupo focal 5 (cinco) se presentó un caso de personas defensoras que sufrieron el intento del robo de WhatsApp a través de un proceso de suplantación de su identidad.

Para concluir, es importante resaltar que, de manera transversal en los espacios de conversación de los grupos focales, las personas participantes expresaron sentirse vigiladas tanto en su trabajo como en su vida personal, ya sea a través de medios digitales o en su día a día. Esta sensación, vinculada al conflicto en zonas rurales y a la histórica persecución que han sufrido las personas defensoras en el país, se entrelaza con el uso de la tecnología. En consecuencia, los incidentes de seguridad digital no pueden comprenderse aislados del contexto de violencia constante al que están expuestas estas personas. Los incidentes de seguridad digital forman parte de una continuidad de agresiones y de un sabotaje intencionado al trabajo que lideran, siendo el resultado no del uso de internet o del acceso a la tecnología, sino de los escenarios de persecución en los que se encuentran.

06. Bibliografía

Alva de la Selva, A. R. (2015). Los nuevos rostros de la desigualdad en el siglo XXI: la brecha digital. Revista Mexicana de Ciencias Políticas y Sociales, 60(223), 265-285.

Centro Nacional de Consultoría. (2023). Apropiación digital 2023. Autor.

Corte Constitucional. (2023). Sentencia SU-546 de 2023. [MP José Fernando Reyes Cuartas]

Defensoría del Pueblo. (2022). Conceptos básicos en derechos humanos y obligaciones de los Estados. Defensoría del Pueblo de Colombia.

Departamento Nacional de Planeación. (2010). Importancia estratégica de la estrategia de gobierno en línea (Documento Conpes 3650). Bogotá D.C., Colombia: Consejo Nacional de Política Económica y Social

Departamento Nacional de Planeación. (2020). Política Nacional de Seguridad Digital y Ciberdefensa: Documento CONPES 3995. DNP.

Franco Avellaneda, M. & Pérez-Bustos, T. (2010). Tensiones y convergencias en torno a la apropiación social de la ciencia y la tecnología en Colombia. En Centro de Innovación para la Apropiación Social de la Ciencia y la Tecnología, Deslocalizando la apropiación social de la ciencia y la tecnología en Colombia: Aportes desde prácticas diversas (pp. 9-23). Convenio Maloka-Colciencias.

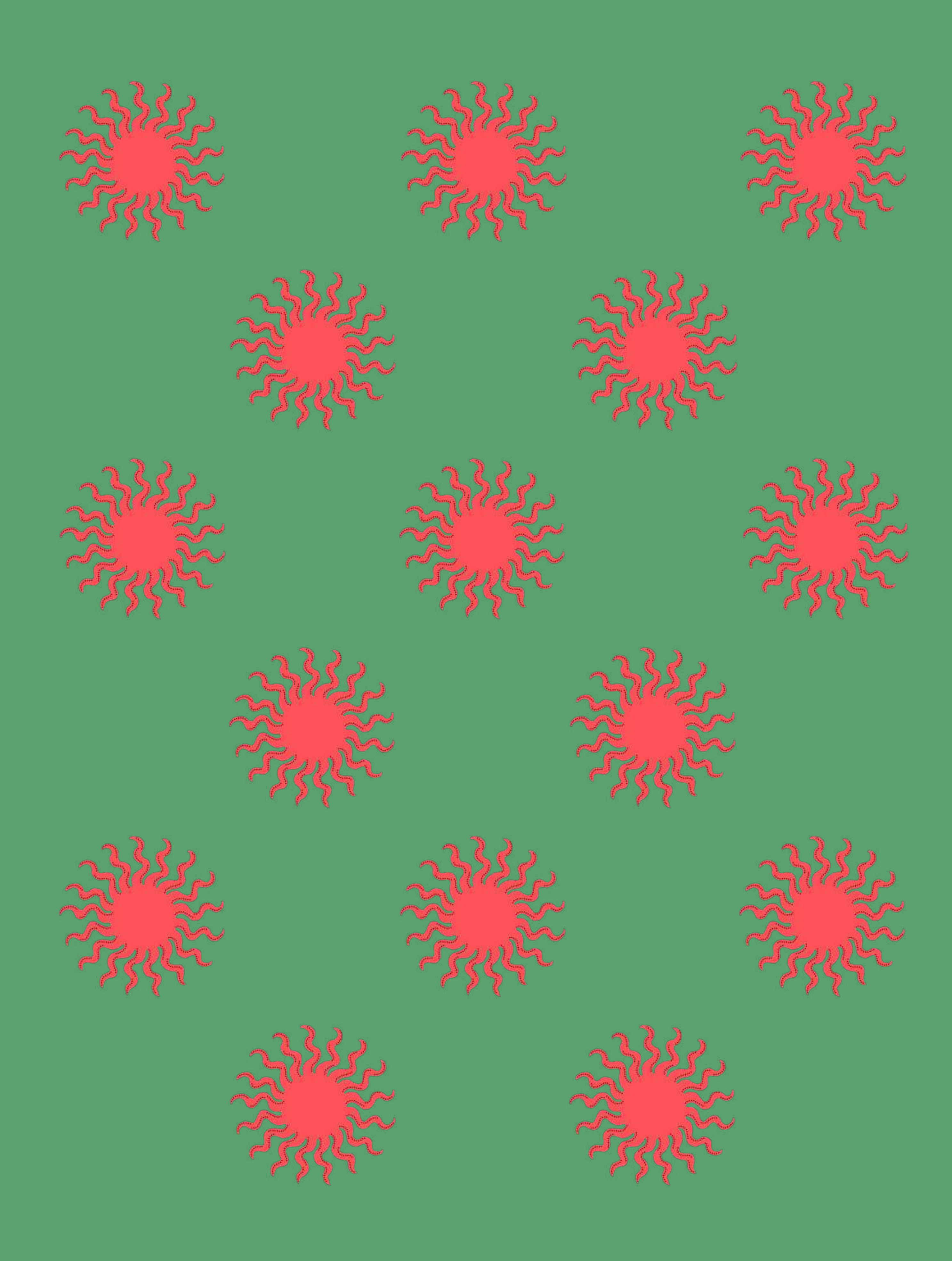
Grillo, O. (2019). Itinerarios de la antropología y su mirada sobre el mundo digital. En A. L. Rivoir y M. J. Morales (Coords.), Tecnologías digitales: Miradas críticas de la apropiación en América Latina (pp. 21-34). Clacso.

Ministerio de Educación Nacional. (s.f.). Manual de políticas de seguridad digital. MEN.

Ministerio de Tecnologías de la Información y las Comunicaciones. (2021). Apropiación digital 3.0: Elevando la conversación de tecnología en Colombia. Documento de Resultados Finales. MinTIC.

Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos. (s.f.). Acerca de los defensores de los derechos humanos. Naciones Unidas.

Pérez de Acha, G. (2018). ¿De qué hablamos cuando hablamos de acceso? Derechos Digitales.




<K+LAB>
Fundación Karisma
@Karisma
Karismacol
fundacion karisma
Karisma.org.co